III. REMARKS

In the specification it is said (page 15, lines 13-17): "Normally a new ciphering mask is produced for each radio frame of the physical layer of the protocol stack. If interleaving is used, then a new ciphering mask can be produced for each interleaving period of the physical layer of the protocol stack. Typically one interleaving period consists of several radio frames."

Interleaving is a well-known concept for the person skilled in the art. The specification defines it as follows (page 7, lines 5-9): "Having been channel encoded, the channels are interleaved in an interleaver 204A, 204B. The object of the interleaving is to make error correction easier. In the interleaving, the bits are mixed with each other in a predetermined fashion, so that transitory fading on the radio path does not necessarily make the transferred information unidentifiable."

It is therefore submitted that there is ample disclosure both of interleaving in general and producing a new ciphering mask for each physical period of the physical layer of the protocol stack.

Thus the rejection of claims 15, 30 and 45 on **35 USC §112**, first paragraph should be withdrawn.

The last step of claim 1 ("using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm"), and the corresponding features in the apparatus claims make the independent claims as a whole novel and non-obvious in view of the prior art.

The Examiner cites column 3, lines 35-37, of Finkelstein: "pseudo-random bit generator is re-initialized during each data frame by using a session key and a frame number". As best understood, the Examiner argues that "session key" of Finkelstein corresponds with "ciphering key" of the current application, and that "frame number" of Finkelstein corresponds with "logical channel specific parameter or transport channel specific parameter". It is respectfully submitted that the latter finding of the Examiner is incorrect. In Table 1 of Finkelstein it is said that the "frame number" is composed of a direction-bit, an overflow counter and an ARQ sequence number. So, "frame number" is clearly a number that changes from frame to frame in that one connection that is ciphered.

The person skilled in the art knows that "logical channel specific parameter or transport channel specific parameter" does not change on a frame by frame basis, as these parameters are defined in the 3GPP (The Third Generation Partnership Project) specifications. These parameters remain the same packet by packet during the whole connection, but they are different for the parallel services of the same user (cf. specification page 2, lines 13-22, for the problem solved by the present invention). The term "logical channel specific parameter or transport channel specific parameter" is a generalization of the features (Radio Access Bearer Identifier, Logical Channel Identifier, Signaling link Identifier and Dedicated Channel Identifier) described in the dependent claims. It is clear to the person skilled in the art without further explanations that these are parameters whose values do not change frame by frame.

Claim 1 recites "using a logical channel specific parameter or a transport channel specific parameter as an additional input

parameter to the ciphering algorithm. Similar language is in claims 16 and 31. As explained above, this is not in Finkelstein. Thus the rejection of claims 1, 2, 5, 9, 13, 14, 16, 17, 20, 24, 28, 29, 31, 32, 35, 39, 43, and 44 under 35 USC 102 on Finkelstein should be withdrawn.

Further, since there is no suggestion of this feature in this reference, these claims are unobvious over it.

Claims 9, 24, 39 (...wherein the plain data includes one RLC PDU from one logical channel and for said logical channel an individual ciphering mask is produced): The Examiner refers to Finkelstein's "sequence number" which is different for each frame (data packet). The present claim 9 clearly talks about an individual ciphering mask per logical channel (referring to earlier claims about logical channel specific parameter). These are two totally different issues. For this additional reason, these claims are patentable.

Claims 13, 28, 43 (MAC layer): The Examiner argues that MAC and "Layer 2" (Finkelstein) are identical. It is true that MAC is normally known to be part of layer 2, but it is also very well known that the layer 2 protocol that Finkelstein is talking about - including ARQ mechanism - is not a Medium Access Control (MAC) protocol, but something above it - normally known as, e.g., RLC (Radio Link Control). Moreover, that referred portion of Finkelstein is talking about ciphering above the ARQ mechanism (i.e., above RLC layer), and MAC is very well known to be below the ARQ mechanism. For this additional reason, these claims are patentable.

Claims 14, 29, 44 (physical layer): The referred portion of Finkelstein does not include any sentence indicating that

ciphering is done in physical layer or for each radio frame of physical layer separately (even on different layer). On the contrary, Finkelstein is always referring ciphering either in layer 3 or layer 2. He only mentions (column 5, lines 33-35) that the encrypted packets are received from the physical layer. Reading that chapter till the end, it is very clearly (even if not explicitly) said that layer 2 generates all the required deciphering parameters and after decryption sends the data packet to network layer. For this additional reason, these claims are patentable.

The Examiner cites an additional reference, US 6,535,979 (Vialén et al.). However, it does not qualify as prior art under 103(c) as the assignee of the reference is the same as in the present application, and because the U.S. filing date of the present application (6 March 2000) is after 29 November 1999. See also MPEP 706.02(k). Further, since Vialen does not disclose using a channel specific parameter as an additional parameter to the ciphering algorithm, even if it is somehow combined with Finkelstein, the result is not the claimed invention.

Thus the rejection of claims 3, 4, 6-8, 10-12, 18, 19, 21-23, 25-27, 33, 34, 36-38 and 40-42 under **35 USC §103** on Finkelstein in view of Vialen should be withdrawn.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

A check in the amount of $110 is enclosed for a one month extension of time and additional claim fees. The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

Henry I. Steckler
Reg. No. 24,139

March 18, 2004
Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date indicated below first class mail in an envelope addressed to the Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Date: 3/22/04

Signature: Carolina Rodriguez
Person Making Deposit